الموسوعة العربية للكمبيوتر/ قسم الدورات التعليمية
سلسلة كتب الدورات التعليمية الإلكترونية
www.c4arab.com

أمن المعلومات
Security



تأليف: الأخ وليد (أبو سعد)

محتويات الكتاب

بالضغط على زر Ctrl **مع أحد محتويات الكتاب، يسهل لك الوصول السريع لها.. وينصح بإظهار شريط الويب** Web **من خلال قائمة العرض** (View) <-- **شريط الأدوات** (Toolbars) <- **شريط الويب** Web، **فمن خلاله ستتمكن من الرجوع إلى صفحة محتويات الكتاب مرة أخرى بالضغط على زر** ..

.. بســــم الله الرحمــــن الرحيــــم ..

الكتاب في سطور

هـذا الكتـاب لـيس فـى الأصـل إلا دورة تـم تدريسـها فـى سـاحة الـدورات التعليميـة بالموسوعة العربية للكمبيوتر والإنترنت ، وتم جمع تلك الـدروس وسلسـلة النقـاش التـى دارت حولها هنا فى هذا الكتـاب ، وتـم وضـع النقاشـات علـى هيئـة أسـئلة وأجوبـة لكـي يستفيد الجميع منها ..

لذلك تعتبر سلسلة كتب الدورات التعليمية :

- **أول سلسلة كتاب إلكترونية عربية خاصة بالمبتدأين.**
- **السلسلة الوحيدة التى تتبع نظام الأسئلة والأجوبة الناتجـة فعـلاً مـن مشـاكل حقيقيـة لأشخاص من مختلف الأماكن والدول ، مما يهيئ عندك نوع من الاستعداد لأي مشكلة قد تواجهها وكيفية التعامل معها.**
- **تعتبر سلسلة الكتاب الوحيدة المدعومـة أربـع وعشـرون سـاعة طـوال العـام ، فيمكنـك الاستفسـار عـن أي مشـكلة وحلهـا عـن طريـق وضـعها فـى سـاحة النقـاش والأسـئلة بالموسوعة .**
- **إن هـذا الكتـاب هـو مـن أجـل نشـر المعرفـة وتوسـيع التفكيـر المنطقـى الأساسـي، فالإحتراف هو ليس الهدف فى حد ذاتـه، بـل الاسـتطلاع واكتشـاف الـذات والإلمـام الجيـد بالأساسيات والمبادئ الأولية من أجل شق طريق النجاح بكل سهولة ويسر.**

التواصل مع القراء

إلى القارئ العزيز ...

حرصت الموسوعة العربية للكمبيوتر والإنترنت .. ومن منطلق اهتمامها العام بعلوم الحاسب والتقنية واهتمامها الخاص بتقديم هذه العلوم باللغة العربية .. على طرح هذه السلسة من الكتب الإلكترونية التى نتمنى أن تحقق طموحات القارئ العربي الذى اعتاد على قراءة أجود المطبوعات بكافة اللغات العالمية .

إن الموسوعة العربية .. من خلال هذه السلسلة .. تطمح لتقديم سلسلة من الكتب بمستوى عالٍ من الجودة ، الشيء الذى لن يتحقق بدون ملاحظاتكم واقتراحاتكم حول السلسلة .. طريقة الكتابة ، الأخطاء الإملائية والنحوية ، التنظيم والترتيب ، طريقة نشر الكتاب وتوزيعه ، الإخراج الفنى ... الخ

ننتظر سماع أراءكم على البريد الإلكتروني المخصص لذلك

ebooks@c4arab.com

نرجو ذكر اسم الكتاب والكاتب والطبعة مع ذكر ملاحظاتكم لنا

الأخت: تـهاني السبيت
مشرفة موقع الموسوعة العربية للكمبيوتر والإنترنت
www.c4arab.com

نبذة عن قسم

الدورات التعليمية



الدورات التعليمية .. هي مجموعة من الدورات التي تقدمها لكم الموسوعة العربية؛ بدأنا بتقديمها في الصيف تحت مسمى " الدورات الصيفية " وها هي تعود من جديد . حرصنا على تقديم دورات في مجالات مختلفة لنراعي أغلب الاهتمامات كما حرصنا على انتقاء الدورات المفيدة، غير المتكررة، بطريقة جادة تنقلك إلى الجو الدراسي في قاعات الجامعة و صفوف المعاهد و لكن في بيئة إلكترونية! كل هـذا مجـانــا! ...

يوجد كذلك ساحة متخصصة لها ضمن مجموعة ساحات الموسوعة العربية للنقاش والأسئلة، تجدها هنـــا! ...



استفد واستثمر وقتك معنا! إذا كنت ترغب في تطوير ذاتك و توسيع نطاق ثقافتك في الحاسوب فاستغل كل دقيقة واستفد معنا! و لا تنسى أننا في عصر المعلومات والسرعة.

ابدأ الآن !انتقل لصفحة الدورات و اختر الدورة التي تناسبك، انتقل لصفحة الأساتذة للاطلاع على قائمة الأساتذة الّذين سيلقون المحاضرات ،انتقل لصفحة التسجيل كي تسجّل نفسك في إحدى الدورات، لن تستطيع المشاركة في أي دورة قبل أن تسجل. انتقل لصفحة المراجع كي تطلع على المراجع المقدمة من الأساتذة بخصوص الدورات الحالية .انتقل لصفحة الملتحقين لتطلع على بعض المعلومات عن الملتحقين في الدورات. انتقل لصفحة اتصل بنا كي ترسل لنا اقتراحاً أو طلباً. نحن بانتظارك! لكن الوقت محدود و عدد الملتحقين في كل دورة محدود لذا لا تتأخر في التسجيل من فضلك.

الدرس الأول [مقدمة]

رابط الدرس الأول: http://www.c4arab.com/showlesson.php?lesid=1755

مقدمة Introduction:

يجلب الارتباط مع شبكة الانترنت تحديات أمنية جديدة لشبكات الشركات الكبيرة، شهد العامان الماضيات دخول آلاف الشركات إلى شبكة الانترنت، حيث أنشأت هذه الشركات مواقع لها على الانترنت، وزودت موظفيها بخدمات البريد الالكتروني ومتصفحات انترنت وأصبح بذلك أمام المستخدم الخارجي المسلح ببعض المعرفة وبعض الأهداف الخبيثة طريقة جديدة للتسلل إلى الأنظمة الداخلية،حالما يصبح هذا الدخيل داخل شبكة الشركة، يمكنه أن يتجول فيها ويخرب أو يغير البيانات، أو يسرقها مسببا أضرارا من مختلف الأنواع ، و حتى إذا أخذنا أكثر تطبيقات الانترنت استخداما وهو البريد الالكتروني فانه لا يعتبر مأمونا ، يمكن لمن لديه محلل بروتوكولات protocol analyzer وإمكانية الوصول إلى الموجهات routers والأجهزة الشبكية الأخرى التي تعالج البريد الالكتروني أثناء انتقاله من شبكة إلى شبكة عبر الانترنت أن يقرأ أو يغير الرسالة المرسلة، إذا لم تتخذ خطوات معينة لضمان سلامتها ، تتصرف بعض الشركات وكأن التحديات الأمنية لم تكن خطرا حقيقيا حيث تتطلع إلى البنية التحتية لشبكة الانترنت، كوسيلة رخيصة نسبيا، لربط شبكتين أو عدة شبكات محلية LAN معزولة جغرافيا مع بعضها البعض أو للربط عن بعد مع شبكة ما.

وتجدر الإشارة إلى أن أعمال التجارية على شبكة الانترنت والتي تتطلب الملايين من التبادلات المصرفية السرية أصبحت قريبة من متناول الكثيرين،وتستجيب أسواق أمن الشبكات Network Security بسرعة لتحديات أمن شبكة الانترنت عن طريق تبني تقنيات التحقق Authentication والتشفير Encryption المتوفرة في هذا المجال لتطبيقها على روابط شبكة الانترنت ، وعن طريق تطوير منتجات جديدة في مجال أمن المعلومات، وتعتبر الأسواق اليوم في فوضى معايير وتقنيات ومنتجات .

السياسات الأمنية Security Policies:

لن يكون الربط مع شبكة الانترنت مثل الربط مع أي نوع آخر من الشبكات آمنا تماما، وبدلا من أن تلجأ الشركات إلى تحقيق الأمن المطلق عليها أن تعرف خطر تسرب المعلومات ، وتحقق نوعا من التوازن بين احتمالات خرق الترتيبات الأمنية وبين كلفة تحقيق مختلق هذه الترتيبات.

يجب أن تركز الخطوة الأولى علي استنباط سياسة أمنية شاملة للشركة أو علي تطوير السياسة الأمنية المتعبة بحيث تأخذ في الاعتبار الربط مع الانترنت ، ويجب أن تحدد هذه السياسة بالتفصيل ، الموظفين الذين يحق لهم الوصول إلى كل نوع من أنواع الخدمة التي تقدمها الانترنت، كما يجب أن تثقف الموظفين في مجال مسئولياتهم تجاه حماية معلومات الشركة مثل مسؤولياتهم تجاه حماية كلمات المرور التي يستخدمونها
بالإضافة إلى تحديد الإجراءات التي ستقوم الشركة بها في حال حدوث خرق لمثل هذه الخطة الأمنية ، وتعتبر هذه السياسة أداة هامة جدا في تحديد المجالات التي ستنفق فيها أموال الشركة للحفاظ علي أمن معلوماتها ، ويقدم كتاب دليل امن المواقع Site Security handbook الذي أصدره مجموعة Network Working Group التابعة لهيئة Internet Engineering task force أو IETF فكرة جيدة عن الموضوعات التي يجب أخذها بعين الاعتبار عند وضع سياسات أمنية.

تتطلب السياسة الأمنية كجزء من ترتيباتها تقدير الكلفة التي ستتحملها الشركة، في حال خرق الترتيبات الأمنية. ويجب أن ينخرط الموظفون علي اعلي المستويات في هذه العملية وقد يكون من المفيد أن تقوم الشركة بتوظيف مستشار لأمن الكمبيوتر، لضمان أمن معلوماتها ، وتقدم الكثير من الشركات المزودة لخدمة الانترنت، الاستشارة والنصح في هذا المجال، وتبدأ بعد تحديد السياسة المتبعة، عملية تقويم استخدام برامج الجدران النارية firewall، والتشفير encryption والتثبت من المستخدم Authentication.

بعض الأمثلة على السياسات الأمنية :

- مسح كلمة السر الخاصة بالموظف المنتهي عقدة فورا(مثلا كإجراء خلال سحب أوراقة من الشركة).
- وضع حساسات Sensors مياه أو حرائق قرب أجهزة تخزين البيانات.
- استخدام الجهاز الخاص بالشركة للانترنت، ويمنع استخدام جهاز غيرة مثلا كأن يحضر laptop .
- لا يسمح بتبادل الرسائل داخل الشركة التي تحتوي على رسائل خاصة أو malicious gossip أو Slander ... .

• صلاحيات كل مستخدم على البيانات الموجودة على قاعدة البيانات .

• الدخول للشركة عن طريق البطاقة الخاصة.

• وضع مثلا أجهزة التحقق من بصمة الشخص على أجهزة البيانات المهمة.





وغيرها الكثير من السياسات الأمنية Security Policies .

أنواع الهجوم Attacks

يقسم الهجوم إلى أربعة أقسام وهي :

1. **هجوم التصنت على الرسائل** Interception Attacks:

وفكره عمل هذا الهجوم: أن المهاجم يراقب الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتصنت على الاتصال (Eavesdropping).

2. **هجوم الإيقاف** Interruption Attacks:

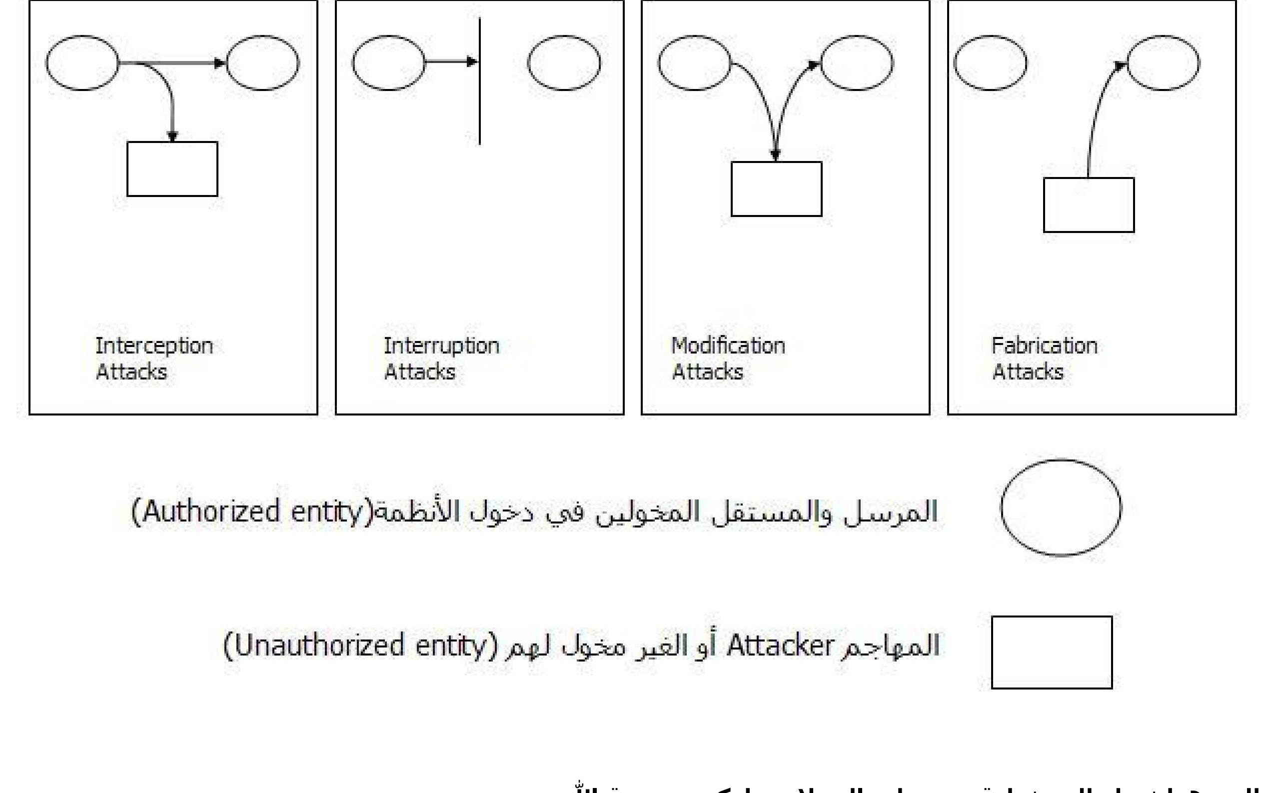
وهذا النوع يعتمد على قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضا برفض الخدمة (Denial of service).

3. **هجوم يعدل على محتوى الرسالة** Modification Attacks:

وهنا يتدخل المهاجم بين المرسل والمستقبل (يعتبر وسيط بين المرسل والمستقبل) وعندما تصل إلى الAttacker فإنه يقوم بتغيير محتوى الرسالة ومن ثم إرسالها إلى المستقبل ، والمستقبل طبعا لا يعلم بتعديل الرسالة من قبل الAttacker.

4. **الهجوم المزور أو المفبرك** Fabrication Attacks :

وهنا يرسل المهاجم رسالة مفادها انه صديقه ويطلب منه معلومات أو كلمات سرية خاصة بالشركة مثلا .



وإلى هنا نصل إلى نهاية درسنا، والسلام عليكم ورحمة الله

****

النقاش والأسئلة

رابط النقاش: http://www.c4arab.com/showthread.php?threadid=25976

لدي سؤالين ..
مافائده أمن المعلومات ؟
وما المقصود بأمن المعلومات؟
بشكل مختصر أختي، أمن المعلومات هو حماية البيانات لمنع وصول الأشخاص الغير مخول لهم الحصول عليها.. وهذه المعلومات أو البيانات سرية وخاصة بالشركة أو المنظمة..

أخي أبو أسعد..
ذكرت من الأمثلة على السياسات الأمنية..
وضع حساسات Sensors **مياه أو حرائق قرب أجهزة تخزين البيانات.**
هل ممكن إيضاح لطريقة الإستفادة منها، بصراحة أراها طريقة بدائية وضعيفة جدا !
فما رأيك..
بالعكس ليست بدائية وهي تضمن مخازن قواعد البيانات من الحرارة بوضع مكيفات وتحسس للحرائق فماذا لو حدث حريق بالقرب من الأجهزة أو تسرب الماء إلى أجهزه البيانات نتيجة الأمطار أو التسربات الأخرى.

قرأت حيث أنشأت هذه الشركات مواقع لها على الإنترنت، وزودت موظفيها بخدمات البريد الإلكتروني ومتصفحات انترنت..
فهل المتصفحات تختلف عن التي نعرفها مثل اكسبلورر و غيره؟
هناك عشرات المتصفحات مثل موزيلا ونت سكيب وغيرها الكثير.

وهل يعني هذا بأن الشركات ستقوم باستعمال أحد هذه المتصفحات أو أنه من الأفضل أن يكون لها متصفحها الخاص؟
لا أغلب الشركات تستخدم الإكسبلورر الموجود مع نظام ويندوز أو موزيلا ونت سكيب مع أنظمة اللينكس.

وبرأيك أي المتصفحات هو الأكثر أمانا ؟
لا يمكني الحكم على أحدها، فكل يدعي الأمن في متصفحه، ولا بد أن يخضع السؤال للبحث الطويل.

ذكرت في الأمثلة:
صلاحيات كل مستخدم على البيانات الموجودة على قاعدة البيانات.
هذه العبارة غامضة فأرجو شرحها شرحا موجزا أو إذا كان بها كلمة ناقصة أو نحوه فأرجو إفادتنا.
لو كان هناك موظفين : المدير والمحاسب مثلا
المدير يطلع على كل الداتا بيس.
المحاسب يطلع على الرواتب فقط.

استفسار آخر..
للرسالة الصادرة وقت الإرسال و للواردة أيضا
هل يمكن اعتبار تناسق الوقت على أنها لم تتعرض لأي هجوم
أم أن هذه النقطة أيضا يمكن التحكم بها من قبل المهاجم ؟
سوف أشرح ما فهمته من السؤال..
مثلا إذا استلمت رسالة من صديقك هل يعني لك شيئا اليوم و الوقت..

ما أقصده هو أنك لو أرسلت لي رسالة الساعة 12.00 **ص على ما أعتقد سوف تستغرق** 10 **ثواني للوصول.. وعندما تتعرض للهجوم سوف تتأخر (الوقت اللازم للمهاجم للتعديل)**
و ليكن دقيقتان وبالتالي ستصلني 12.02 **ص**
فهل بذلك أستطيع أن أحكم بأنها قد هوجمت أم ليس هناك اعتبارا لهذا التخمين ؟
ليس شرطا..
يمكن أن ترسل رسالة وتستغرق أكثر من 10 ثواني.
بسبب زحمة ال Traffic من راوترات وسويتشات ولا يمكننا الإستدلال عليها..
وهي بالأصل لو عمل sniffing لن تتأخر الرسالة.

الدرس الثاني [تعريف الخطر Risk وأقسامه]

رابط الدرس الثاني: http://www.c4arab.com/showlesson.php?lesid=1756

وبعد أن أخذنا مقدمة عن أمن المعلومات لابد لنا من معرفة :

1. تعريف الخطر Risk وأقسامه.
2. الإجراءات المضادة عند حدوث الخطر Countermeasures.
3. كيفية إدارة الخطر و احتمال حدوثه .

سندرس اليوم النقطة الأولى، وندرس النقطتين التاليتين في الدرس القادم إن شاء الله..

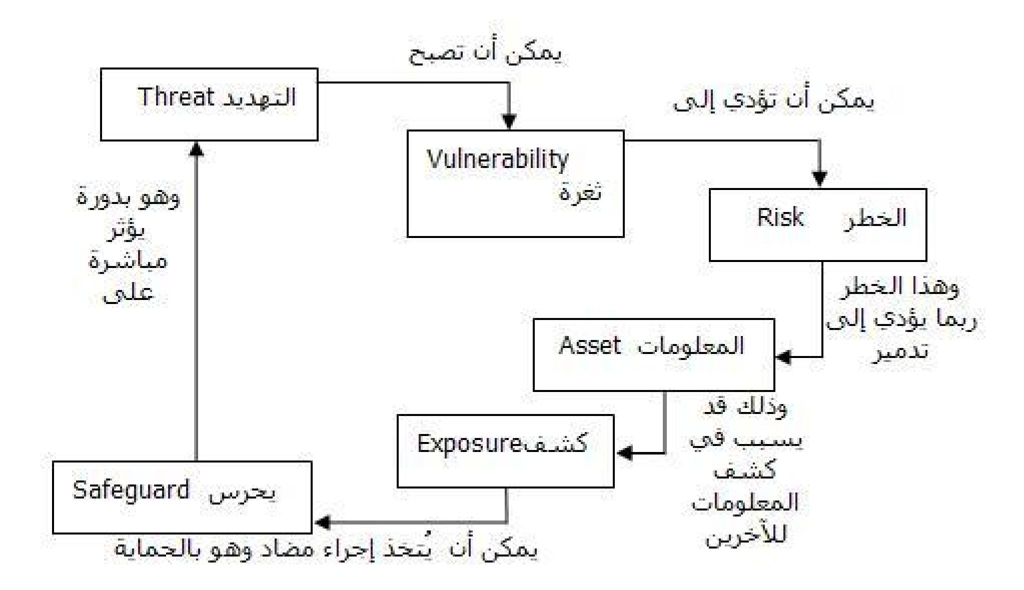
تعريف الخطر Risk وأقسامه:

الخطر أو Risk هو أنه يوجد على الأرجح تهديد يمكن إستغلاله ، وبالتالي إذا استغل ذلك التهديد يمكن أن نطلق عليه Vulnerability (ثغرة) ، حيث أنه يوجد ثغرة أمنية في تلك المنظمة.

ومن هذا التعريف يمكن أن نقسم ال Risk إلى قسمين رئيسيين هما :

- التهديد (Threat) : وهو عملية المحاوله الى الوصول إلى المعلومات السرية الخاصة بالمنظمة.
- الثغرات (Vulnerabilities) : وهي أنه يوجد ضعف في المنظمة يستطيع المهاجم Attacker الدخول من خلالها .

وهناك مكونات أخرى لل Risk وهي كما يوضح الشكل التالي :



والآن سوف نأخذ الـ Vulnerabilities والـ Threats بشيء من التفصيل :

أولا الثغرات Vulnerabilities:

تتكون من نوعين وهما:

- تحصين تقني Technical Vulnerability: إذا كان التحصين ضعيفا واستغل الضعف من قبل المهاجم Attacker يعرف هذا الهجوم بما يسمى بالهجوم التقني.

• تحصين غير تقني Administrative Vulnerability: وهو ما يسمى بالهجوم الغير تقني أو هجوم الهندسة الاجتماعيةsocial engineering Attack.

ويمكن تقسيمها من حيث الصعوبة والسهولة إلى قسمين:

• تحصينات ضعيفةHigh-level Vulnerability: وهو سهل الاستغلال، ومثال عليه كتابه كود برمجي لاستغلال تلك الثغرة.

• تحصينات قوية Low-level Vulnerability : وهذا النوع صعب الاستغلال ويتطلب الكثير من المصادر ، مصادر ماليه أو وقت طويل على المهاجم Attacker.

ثانيا التهديد Threat :

هناك ثلاث مكونات أساسيه للتهديد Threat وهي :

• الهدف Target: وهي المعلومات المراد سرقتها.
• الطريقة أو العميل Agent: وهي الأشياء المكونة والمنشأة للتهديد.
• الحدث Event :وهي نوعية التأثير لوضعية التهديد .

ولنتحدث عن كل منهم بالتفصيل:

1. الهدف Target :

وهي المعلومات الخاصة بالمنظمة ويمكن للمهاجم Attacker بعمل الآتي على كل من :
• الخصوصية Confidentiality: وذلك بكشف المعلومات السرية للآخرين.
• سلامه المعلومات Integrity: يمكنه تغيير المعلومات الخاصة بالمنظمة.
• التواجد Availability : بواسطة رفض الخدمة عن طريق DoS.
• قابلية محاسبة المهاجمAccountability : لكي لا يحاسب المهاجم Attacker فإنه يقوم بإخفاء الهجوم (على سبيل المثال تغيير سجل الأحداث Events logs).

2. الطريقة Agents(أو العميل):

لابد من توفر ثلاث سمات :
• الوصول إلى الهدف Access to the target: قد يكون وصول مباشرDirect (أي أن لدية حساب دخول على النظام وقد يكون غير مباشر Indirect (وذلك بالدخول عن طريق وسيط).
• معلومات عن الضحية Knowledge about the target.
• الدوافع أو أسباب الهجوم Motivation.

3. الأحداث Events:

وهي تكون بطرق عديدة من أهمها إساءة الدخول المخول Authorized وغير المخول Unauthorized إلى المعلومات أو النظام.وإما عن طريق وضع أكواد خبيثة Malicious (تروجونات أو فيروسات) في الأنظمة.

و إلى هنا نصل إلى نهاية الدرس الثاني ونكمل ما تبقى لنا من عناصر في الدرس القادم إن شاء الله.

ولا تنسونا من الدعاء .

****

النقاش والأسئلة

رابط النقاش: http://www.c4arab.com/showthread.php?threadid=26002

ما هي الثغرات ؟
الثغره نتيجة نقص في برنامج(خلل) فكم نسمع عن الثغرات في نظام ويندوز.

هل عملية التهديد تحاول إيجاد أو خلق ثغرات ؟
إذا كان هناك ثغرة أمنية في الأنظمة فإنها تشكل تهديد.

ممكن توضيح حول:
التواجد : Availability **بواسطة رفض الخدمة عن طريق** DoS.
مثال عليه : مثلا عندما تطلب موقع وتظهر لك رسالة بوجود زيادة الطلب على الموقع. أو إن الموقع تم اختراقه ومسحت جميع بياناته.

هل تقصد أستاذنا مثل ما حدث مع بعض المواقع الإخبارية والسياسية والحكومية في فترة الحرب على العراق (ومنها على ما أذكر الجزيرة نت و موقع البيت الأبيض) ؟
أخي الذي أصاب موقع الجزيرة يطلق عليه redirect

وما هي آلية الـ redirect **وبماذا يختلف عن الـ**Availability ..؟
أخي : redirect هي عمليه سهلة كالذي حدث لموقع الجزيره عندما تطلب موقع الجزيره فهو اتوماتيكيا يحولك على موقع وضعه أشخاص (هي عمليه تحايل على أجهزة الـback bone بأن هذا الموقع هو موقع الجزيره)
أما التواجدية: هو أن هذا الموقع لا يكون موجود وقت الطلب .

سؤال آخر : **هل رفض الخدمة** DoS **هو المصطلح الذي أخذناه بالدرس السابق**(denial of service)
هو رفض الخدمة (DoS) بالتأكيد هو اسم عندما يصاب الموقع بزيادة الطلب.

ممكن توضيح .. social engineering attack **؟؟**!!
هجوم الهندسة الإجتماعية: هي بأوضح مثال : عندما يقوم شخص بالإتصال على Administrator ويدعي أنه مدير القسم ويقول لقد نسيت كلمه السر الخاصة بي هلا أرسلتها لي مثلا.

في target **التواجد ورفض الخدمة المقصود بها هو إيقاف الخدمة التي يقدمها الموقع المخترق للمستخدمين؟**
أعتقد تم شرحه.

في accountability **كيف يمكن محاسبة المخترق ومعرفة شخصيته ... أم أن المقصود هنا هو فقط كشف الإختراق.. ؟**
بالنظر الى ال log file لمعرفة الداخلين على النظام (مثال) وهناك أكثر من طريقة .

لكي لا يحاسب المهاجم Attacker **فإنه يقوم بإخفاء الهجوم (على سبيل المثال تغيير سجل الأحداث** (Events logs
هل يمكن مزيد من التوضيح في هذه النقطة..
إخفاء الأثر من أصعب العمل الذي يقوم به المهاجم..
عندما يخترق الهاكر موقع يسجل ال IP الخاص في الـ log file
وبالتالي يستخدم الهاكرز بعض الحيل مثلا تغيير ال IP أو الدخول عن طريق جهاز مصاب ويتحكم به الهاكر ليشن به الهجوم على الـtarget

هل المقصود في تحصينات ضعيفة: High-level Vulnerability **وهو سهل الاستغلال، ومثال عليه كتابه كود برمجي لاستغلال تلك الثغرة ..**
هو مثلما تتخذه بعض المنتديات في منع كود ال HTML **للحماية من الثغور؟؟**
ربما إذا كان يوجد ثغرات.

كثيرا ما سمعت عن مصطلح ثغرة Exploit = **فهل هو صحيح ؟**
وإذا كان صحيحا فهل هناك فرق بين الـ Exploit **و ال** Vulnerability **؟**
ال Vulnerability تعتبر ثغرة بينما ال Exploit الإستغلال .. طريقة استغلال الثغرة سواء برنامج، قطعة كود أو طرق أخرى .. وأحيانا تطلق على الكود نفسها ..

أرجو أن تقوم بضرب أمثلة على التحصين التقني والتحصين الغير تقني ؟
التحصين التقني: استخدام الأجهزه للحمايه مثل أجهزة التشفير.
التحصين الغير تقني : مثل برامج الجدران النارية و مضادات الفيروسات.

الدرس الثالث [الإجراءات المضادة عند حدوث الخطر Countermeasures]

رابط الدرس الثالث: http://www.c4arab.com/showlesson.php?lesid=1757

وبعد أن عرفنا تعريف الخطر Risk وأقسامه نكمل ما تبقى لدينا :

2. الإجراءات المضادة عند حدوث الخطر Countermeasures.
3. كيفية إدارة الخطر و احتمال حدوثه .

الإجراءات المضادة عند حدوث الخطر Countermeasures:

لا شك أن المعلومات تختلف من منشأة إلى منشأة وعلى حسب أهمية المعلومات فأن المنشأة تتخذ الإجراء المناسب ، وقد يكون التدخل قبل حدوث الخطر ويسمى Proactive Model وقد يكون تدخل بعد حدوث الخطر (انفعالي أو عاطفي) ويسمى Reactive Model. وسنقوم بشرحه لاحقا.

وهنا بعض أمثلة الإجراءات المضادة للتهديد Threats أو الهجوم Attacks:

- وضع جدران نارية Firewalls.
- برامج مكافحة الفيروسات Anti-virus software.
- التحكم بالدخول Access Control.
- مضاعفة أنظمة التحقق من المستخدم Two-factor authentication systems.
- التدريب الجيد للموظفين Well-trained employees.

وغيرها الكثير من الإجراءات.

كيفية إدارة الخطر و احتمال حدوثه:

الخطوات المتبعة في إدارة الخطر Risk هي:

أولا: تحليل الخطر (Risk Analysis).

ثانيا: اتخاذ قرار بشأن هذا الخطر (Decision Management).

ثالثا: تطبق ذلك القرار (Implementation).

ويوضحها الشكل التالي:



إدارة الخطر من حيث التدخل ينقسم إلى قسمين هما:

1. تدخل بعد حدوث الخطر Reactive Model: وهذا النوع مشهور جدا وهو ما يسمى بالتدخل الانفعالي أو العاطفي Emotional، على سبيل المثال يقوم مسئول الأمن في الشركة بتحميل برنامج مكافح الفيروسات بعدما ينتشر الفيروس ويدمر بعض الأجهزة ويمكن حسابه كما يلي :

تكلفة الحماية = مجموع تكلفة هذا الخطر + تكلفة الإجراء المضاد.

2. يستعد للتدخل أي قبل حدوث الخطر Proactive Model: وهذا النوع أفضل بكثير من ناحية التكلفة، حيث يقلل من تكلفة الخطر. كما يلي:

تكلفة الحماية = الحد الأدنى من الخطر + تكلفة الإجراء المضاد.

والآن ننتقل لحساب احتمالية حدوث التهديد Threat:

الخطوات المتبعة لحساب الاحتمالية هي كما يلي :

1. البداية من أعلى أي أنها على شكل شجري Tree.

2. البحث عن الطرق المؤدية أو المحتملة إلى وقوع التهديد.

3. جمع هذه الطرق باستخدام العلاقات (AND,OR,XOR).

4. لحساب الاحتمالية فإننا نبدأ من أسفل إلى الأعلى.

شرح بعض هذه العلاقات (AND,OR):

P(A)
P(B)
P(A)*P(B)
AND

P(A)
P(B)
P(A)+P(B)-P(A)P(B)
OR

الحدث (Ultimate cause)

وهذه العلاقات تمثل:

AND: (لا بد من تحقق فرعين متوازيين من ال Tree معا).

OR: (أن يتحقق أحد الفرعين المتوازيين).

وبالمثال يتضح المقال:

عندما يحاول المهاجم Attackers كسر كلمة السر الخاصة بال Root.

- إما أن يحاول المهاجم معرفة كلمة ال Root بالتخمين Guessing the root password .

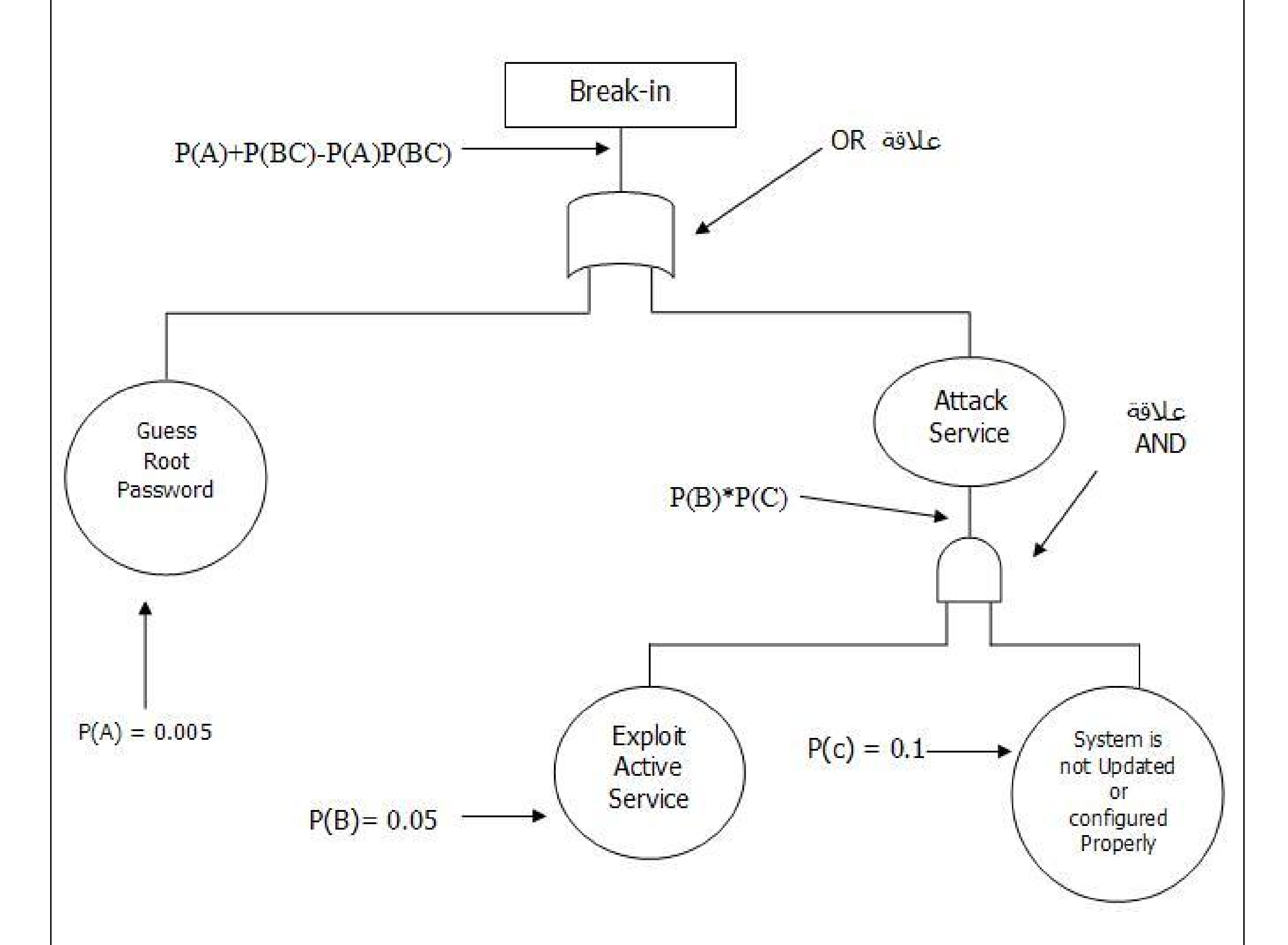
- أو مهاجمة الشبكة ككل لمحاولة وجود Bugs في الشبكة .

ويندرج تحت هذه النقطة عنصرين لتحقق وجود Bugs وهي :

1. أن يوجد ثغرات يمكن استغلالها AND و أيضا لابد أن يتحقق الشرط التالي مع هذا الشرط.

2. أن لا يحدث النظام (أي لا تمحل ترقيعه Patch لهذه الثغرة).

وبعد ذلك نقوم بتمثيل هذه العملية على الـ Tree:



مع الفرضيات التالية:

- P(guessing root password = A) = 5/1000 = 0.005،
- P(exploiting ((استغلال active server = B) = 50 /1000 = 0.05 AND
- P(system is not updated or not configured properly =C) = 0.1

في هذه الفرضيات جعلنا تخمين كلمه السر تساوي A.واستغلال الثغرة جعلناها تساوي B والأخيرة إذا لم يُحدث النظام تساوي C.

لتسهيل عملية الحساب عليها بدلا من الأسماء الطويلة .

سوف نقوم بتوضيح بعض الخطوات في الشكل السابق :

ولحساب الاحتمالية :

P(attack service =BC) = P(B)*P(C) = 0.05 * 0.1 = 0.005 (AND من الـ)

P(break-in = (أي الكلي P(A)+P(BC)-P(A)P(BC) = 0.005+0.005 – 0.005 *0.005 = 0.009975 (OR من الـ)

إذا الاحتمالية الكلية (break0in) هي 0.009975 .

و إلى هنا نصل إلى نهاية الدرس الثالث.

ولا تنسونا من الدعاء .

****

النقاش والأسئلة

رابط النقاش: http://www.c4arab.com/showthread.php?threadid=26021

أخي أبوسعد هل ممكن أن تشرح النقطة التالية
(البداية من أعلى أي أنها على شكل شجري Tree)
أنظري إلى المثال:
ستلاحظين أن في الأعلى رأس واحد كما في الشجرة ويوجد في الأسفل جذور (كثيرة كما في المثال)

p(A) = 5/1000
p(B) = 50/1000
p(C) = .1
لماذا ؟
هذه عملية يحددها خبير أمن المعلومات
مثلا :لنفترض في قوه ال : root password
إذا كانت ضعيفة مثل 123456789 فإن احتمالية كسرها تساوي 0.6 .
وإذا كانت قوية مثل ~z-e=r%vy#y9 فإن احتمالية كسرها تساوي 0.00001

كيف تم حساب المعلومات السابقة ؟
لو نظرت إلى المثال:
على حسب ضعف أو قوة كلمة السر وهي إلى حد ما تقريبية.

في هذه النقطة:
- P(guessing root password = A) = 5/1000 = 0.005،
- P(exploiting ((**استغلال** active server = B) = 50 /1000 = 0.05 AND
- P(system is not updated or not configured properly =C) = 0.1

في هذه الفرضيات جعلنا تخمين كلمه السر تساوي.A **واستغلال الثغرة جعلناها تساوي** B **والأخيرة إذا لم يُحدث النظام تساوي.**C
هل ممكن أن تشرح لنا العلاقات و إلى ما ترمز ؟
ال P اختصار لل Probability الإحتمالية..
أما ال A,B رموز تمثل الحدث كما هو مبين في الدرس.

ممكن أخي أن تكتب خلاصة للقوانين التي يجب أن نستخدمها في حساب البيانات السابقة ؟
أية قوانين!!..
أنظر لأول رسمة خاصة بـAND و OR هذه هي القوانين.

هل يمكن أن يعد هذا القانون قانونا لحساب الإحتمالية:
P(A)+P(BC)-P(A)P(BC) **؟؟**
نعم أخي..
هذا هو القانون الأساسي..
وإن شاء الله بالأمثلة القادمة ستتضح النقطة أكثر.

مثال ثاني على حساب الاحتمالية:
http://www.c4arab.com/courses/common/images/2
ملاحظة: الصورة غير متوفرة

رابط المثال: http://www.c4arab.com/courses/common/images/2ndExample.htm

هل تعتبر ال Tree **الموجودة في الدرس هي قالب ثابت نقوم بملئ البيانات بها كما في المثال**: **لحساب احتمالية حدوث التهديد** ... Threat **؟؟**
لا يا أخي..
على حسب ال Problem لدينا ...كل مشكله ولها شكل خاص فيها.

إذا كيف يمكن تحديد الـ Tree **الخاص بكل مشكلة ؟**
وهل ممكن مثال آخر غير ما ذكر حتى تتضح الصورة؟
خطوات حلها موجوده في الدرس وإن شاء الله سيكون هناك مثال آخر.

هل عملية الاختراق عملية مستمرة أم لحظية بحيث تتم في مرة واحدة فقط ؟
وإذا كانت لحظية فلماذا علينا أن نتأكد من أنه لن يحدث ترقيع للنظام فيما بعد ؟
عمليه الاختراق تتم في أي وقت ..
وتحديث الأنظمة لابد منه ويتحتم مع وجود ثغرة في النظام.

بما أن الاختراق يحدث في لحظة..
فلماذا نهتم بوجود ترقيع للثغرة فيما بعد والتي تم استعمالها في الاختراق ؟
اللحظة لا يمكن تحديدها في وقت محدد..
الثغرة قد لا تكون معلومة من قبل المنظمة إلا في وقت قد يكون متأخر..
والثغرة ليست واحدة..
قد تغلق الثغرة ..وعند تحميل بعض البرامج ينتج ثغرة أخرى.

هل من الممكن أن تكون احتمالية حدوث الخطر = 0
و إذا كان لا، فما هو أقل رقم يمكن تحقيقه مع افتراض وجود كل الإمكانيات ؟
لا..
لا يمكن ذلك فهى عملية مستحيلة .. ممكن أن يحدث الهجوم من داخل المنظمة وقد يحدث من خارجها.
أقل رقم هو بزيادة الحماية. كلما زادت الحماية قلت احتمالية الخطر.

الدرس الرابع [التشفير (1) Encryption]

رابط الدرس الرابع: http://www.c4arab.com/showlesson.php?lesid=1758

مقدمة Introduction :

التشفير أو (التعمية) استخدم قديما في الحضارات القديمة لإخفاء المعلومات والمراسلات مثل الحضارة الفرعونية والدولة الرومانية. ولكن التشفير كعلم مؤسس منظم يدين بولادته ونشأته للعلماء الرياضيين واللغويين العرب إبان العصر الذهبي للحضارة العربية ومن أشهرهم الفراهيدي والكندي، وقد ألف هؤلاء العلماء مفاهيم رياضية متقدمة من أهمها التوافيق والتباديل . وكذلك توظيف الكندي ومن تبعه مفاهيم الإحصاء والاحتمالات في كسر الشفرة ، وقد سبقت هذه الكتابات كتابات باسكال وفيرما بحوالي ثمانية قرون !!!

وقد شاع في أيامنا استخدام مصطلح "التشفير" ليدل على إخفاء المعلومات. ولكن كلمة "التشفير" وافدة من اللغات الأوربية (Cipher) وهذه بدورها جاءت أصلا من اللغة العربية ولكن بمعنى آخر لكلمة "الصفر". فكما هو معلوم أن العرب قد تبنوا مفهوم الصفر والخانات العشرية واستخدموه في الحساب، وهو ما لم يكن الأوربيون يعرفونه في القرون الوسطى ، وكان مفهوم الصفر جديدا وغريبا لدرجة أنهم أخذوه بنفس الاسم فأسموه "Cipher". ولأن مفهوم الصفر الجديد كان في منتهى التعقيد والغموض فقد صاروا يستخدمون كلمة "Cipher" للدلالة على الأشياء المبهمة وغير الواضحة.

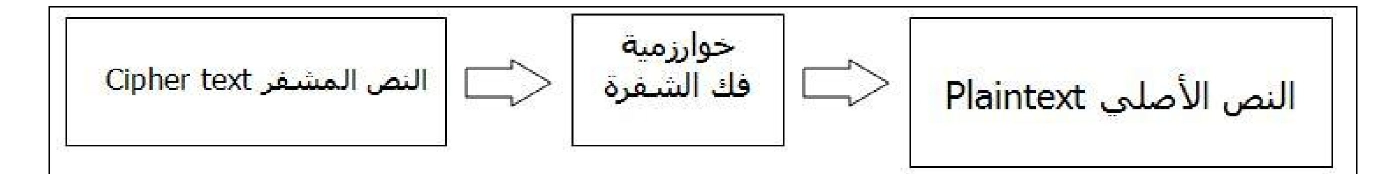
ومن هنا تطور استخدام كلمة "Cipher" في جميع اللغات الأوربية تقريبا لتعني إخفاء المعلومات وقمنا – نحن العرب- بعد ستة قرون بإعادة بضاعتنا الأصلية ولكن بمعنى مختلف فنحتنا كلمة غريبة على اللغة العربية هي "التشفير".

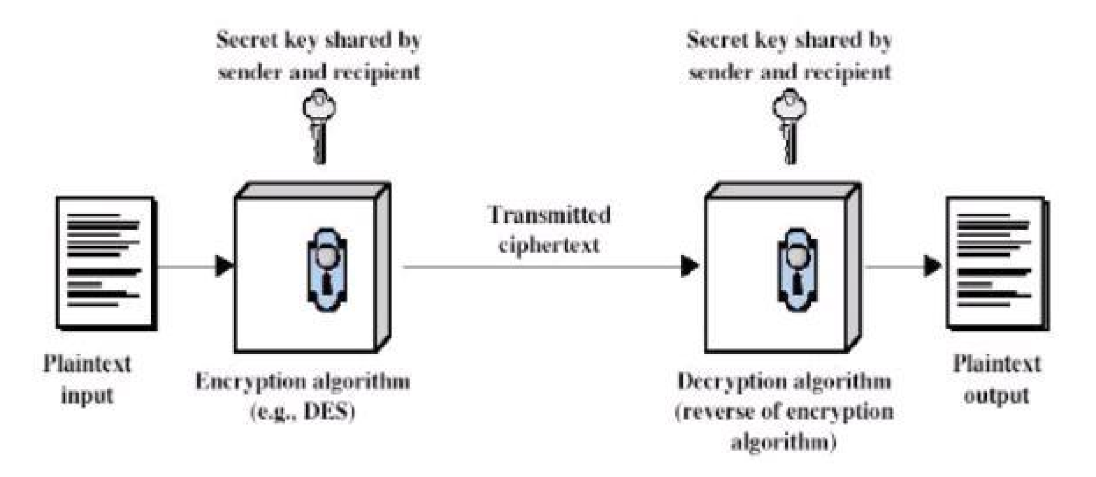
تمهيد

التشفير: هو تحويل المعلومات المهمة أو التي لا تريد أن يطلع عليها أحد إلى نص مخفي(أي لا يمكن فهمه).

النص الأصلي Plaintext ⇦ خوارزمية تشفير النص ⇦ النص المشفر Cipher text

وعملية فك التشفير كالتالي:





وكمثال بسيط على ذلك نأخذ على سبيل المثال كلمة Arab الخطوات أو الخوارزمية لتشفير تلك الكلمة:
نجعل كل حرف يساوي الحرف الذي تليه أي أن:

A = B

R = S

A = B

B = C

وفي هذا المثال النص الأصلي Plaintext هو Arab والنص المشفر هو BSBC وبذلك قد أخفينا النص الأصلي وعندما تصل إلى الطرف الثاني فإنه يقوم بعكس التشفير أي أننا :

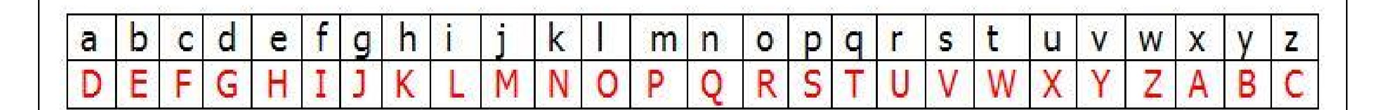
نجعل كل حرف يساوي الحرف السابق ، وبذلك قد حصلنا على النص الأصلي.

وسوف نتطرق إلى بعض الطرق المتبعة في التشفير إن شاء الله، وهي:

- طريقة Caesar
- طريقة Monoalphabetic
- طريقة Playfair
- طريقة Vigenere

• طريقة Caesar :

وهي من أبسط طرق التشفير وهذه الطريقة تعتبر من أقدم طرق التشفير، وفكرة هذه الطريقة هي تبديل كل حرف بثالث حرف بعده مثلا((A=D. وهكذا، وهذا الجدول يوضع جميع الحروف:



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

الشرح :

لنأخذ على سبيل المثال النص الأصلي Plaintext هو "C for Arab" ونريد تشفيره، نقوم بتبديل كل حرف بثالث حرف بعده:
كما هو واضح في الجدول السابق فإن ثالث حرف بعد ال C هو F ، وثالث حرف بعد ال F هو I ، وهكذا إلى أن ينتج لنا النص المشفر Ciphertext:

"F IRU DUDE"

مثال آخر:

Meet me after the party

والنص المشفر Cipher Text:

PHHW PH DIWHU WKH SDUWB

عيــــــوب هذه الطريقة :

1.لو نظرنا إلى هذه الطريقة من جانب أمني لرأينا أنها سهلة الكسر لدينا 26 احتمالية (عدد الحروف الانجليزية) أو بالأصح 25 احتمالية لأن الحرف لا يساوي نفسه .
ولنأخذ على سبيل المثال الحرف A لكسره نجرب كل الحروف ماعدا الحرف نفسه وهذه طريقة معروفه لكسر التشفير وتسمى البحث الشامل Brute force Search .

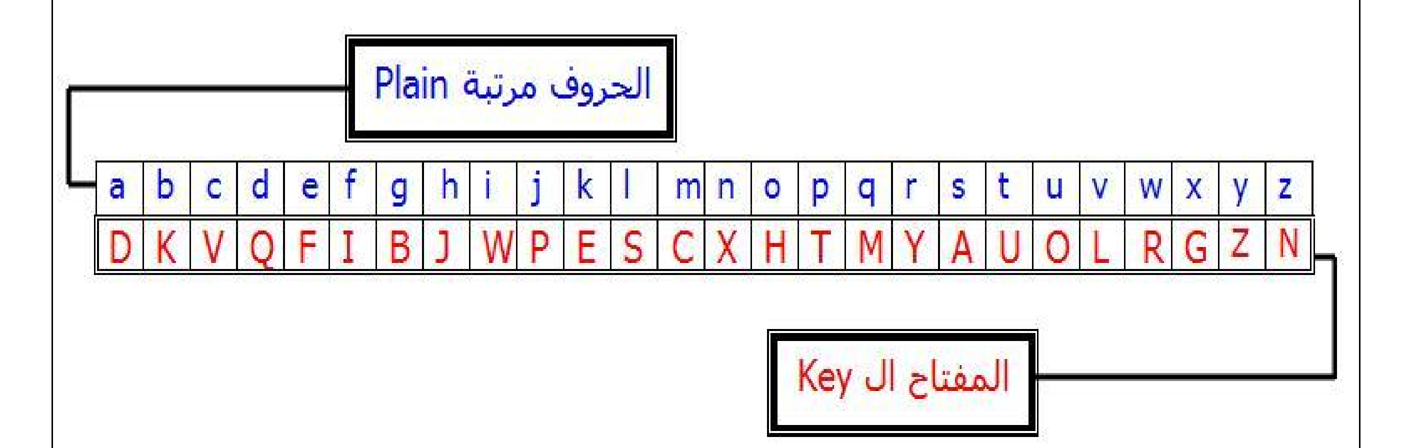
2. لا يوجد مفتاح Key، وسوف نرى في الطرق الأخرى فائدة المفتاح أي أن هذه الطريقة ثابتة،(نقوم بإرسال النص المشفر فقط).

- **طريقة** Monoalphabetic :

فكرة هذه الطريقة أن يكون لدينا مفتاح Key ونقوم بتبديل النص الأصلي بالمفتاح Key.وهي أفضل من طريقة Caesar لأن المفتاح متغير :

الشرح:

لدينا الأحرف من a-z:



سؤال: لماذا قمنا باختيار هذا المفتاح (DKVQFIBJWPESCXHTMYAUOLRGZN) **هل له قاعدة ؟**
الجواب: نحاول أن نختار المفتاح عشوائيا، و ليس له قاعدة قمنا باختياره عشوائيا ونحاول أن نوزع الحروف بشكل متباعد.

والآن وبعد أن و ضعنا المفتاح ال Key ونريد تشفير رسالتنا بذلك المفتاح ولنفرض أن الرسالة plaintext التي لدينا هي : "C for Arab" .

ولتشفيرها : نبدأ بحرف C ننظر إلى الحروف Plain ونبحث عن الـC و نرى ماذا يقابله (في الجدول السابق) ، ويقابلة حرف الـV . ثم نأتي للحرف التالي وهو ال f وننظر لمقابلة في الجدول وهو حرف الـ I .... وهكذا إلى أن نحصل على النص المشفر Cipher text :

"V IHY DYDK"

مثال أخر:

النص الأصلي:

Plaintext: ifwewishtoreplaceletters

والمفتاح كما في الجدول السابق، ناتج التشفير:

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

و إلى هنا نصل إلى نهاية الدرس الرابع.
ولا تنسونا من الدعاء .

****

النقاش والأسئلة

رابط النقاش: http://www.c4arab.com/showthread.php?threadid=26043

ذكرت في بداية تعريف التشفير المصطلح " DES " فماذا تقصد به؟
الـ DES اختصار للــ.. Digital Encryption Standard
وهي طريقة تشفير متقدمة.

طريقة Monoalphabatic كيف يكون key متغير وهل يتم إعلام المستقبل عند تغييره في كل مرة ؟
الجواب : موجود في الدرس:

نحاول أن نختار المفتاح عشوائيا، و ليس له قاعدة قمنا باختياره عشوائيا ونحاول أن نوزع الحروف بشكل متباعد .

أي نختار الحروف عشوائيا بالشروط السابقة.

نعم أفهم هذا ولكن هل كل مرة سوف يتم إرسال المفتاح الذي تم اختياره للمستقبل حتى يقوم بفك الشيفرة على أساس المفتاح الجديد الذي تم اختياره ؟
نعم بالاتفاق بين المرسل والمستقبل على الـKey

1. لو نظرنا إلى هذه الطريقة من جانب أمني لرأينا أنها سهلة الكسر لدينا 26 احتمالية (عدد الحروف الانجليزية) أو بالأصح 25 احتمالية لأن الحرف لا يساوي نفسه .
ولنأخذ على سبيل المثال الحرف A لكسره نجرب كل الحروف ماعدا الحرف نفسه وهذه طريقة معروفه لكسر التشفير وتسمى البحث الشامل Brute force Search .
السؤال: ألا ينطبق نفس الكلام على طريقة Monoalphabatic وبذالك تصبح هي أيضا سهلة الكسر؟
لا أختي :
في طريقة : Caesar ترتيب الحروف ثابت ال a بعده ال b وهكذا .
أما في طريقة : Monoalphabetic ترتيب الحروف غير ثابت مثلا لنأخذ ال a فلا ندري أي حرف بعده.

أستاذ أبو سعد نحن نتحدث على من يحاول فك الشفرة ولا يعلم شيء عن طريقة التشفير المستخدمة فيحاول فك الشفرة عن طريف البحث الشامل وهي تجريب كل حرف مع جميع الحروف ال 25 الباقية ... وهكذا حتى يصل الى فك الشفرة .
لا هناك فرق بين الطريقتين :
في : Caesar لو عرف تحويل حرف واحد فقط سوف يتمكن من حل الشفرة بالكامل .
اما في : Monoalphabetic لو فك حرف واحد فقط لن يتمكن من فك البقية.

(نقوم بإرسال النص المشفر فقط)
أيضا في طريقة Monoalphabatic نقوم بإرسال النص المشفر فقط ؟
نعم هو كذلك.

لم ألاحظ وجود الفراغ (Space) و الأرقام هل هي قاعدة أم أنه يمكننا إدراج أي رقم أو رمز و وضع مفتاح لها بهذه الطريقة ؟
أخي أي أرقام وأي مسافات وضح لو سمحت!!..

أستاذي الغالي أبو سعد
في المثال الأول لدينا النص الأصلي C for Arab
و المشـــفر V IHY DYDK
لماذا لم يتم وضع مقابل للفراغ في المفتاح بدلا من أن ينقل كما هو ؟
لا.. المسافات ليس لها معنى فقط للتوضيح إن شئت
فعلت CforArab
وينتج VIHYDYDK

الدرس الخامس [التشفير (2) Encryption]

رابط الدرس الخامس: http://www.c4arab.com/showlesson.php?lesid=1759

وبعد أن عرفنا طريقة Caesar وطريقة Monoalphabetic، قد يتبادر إلينا أن طريقة Monoalphabetic قوية بما فيه الكفاية ، وهذا ليس صحيح !!!

تكمن المشكلة في أن اللغة فيها تكرار (سواء اللغة العربية أو اللغة الإنجليزية) ولنأخذ على سبيل المثال " th lrd sm allh shll nt wnt" .

ولفهم المثال السابق لا يلزمنا كتابة الحروف كاملة بل فهمناها بحذف حروف العلة (Vowels) .

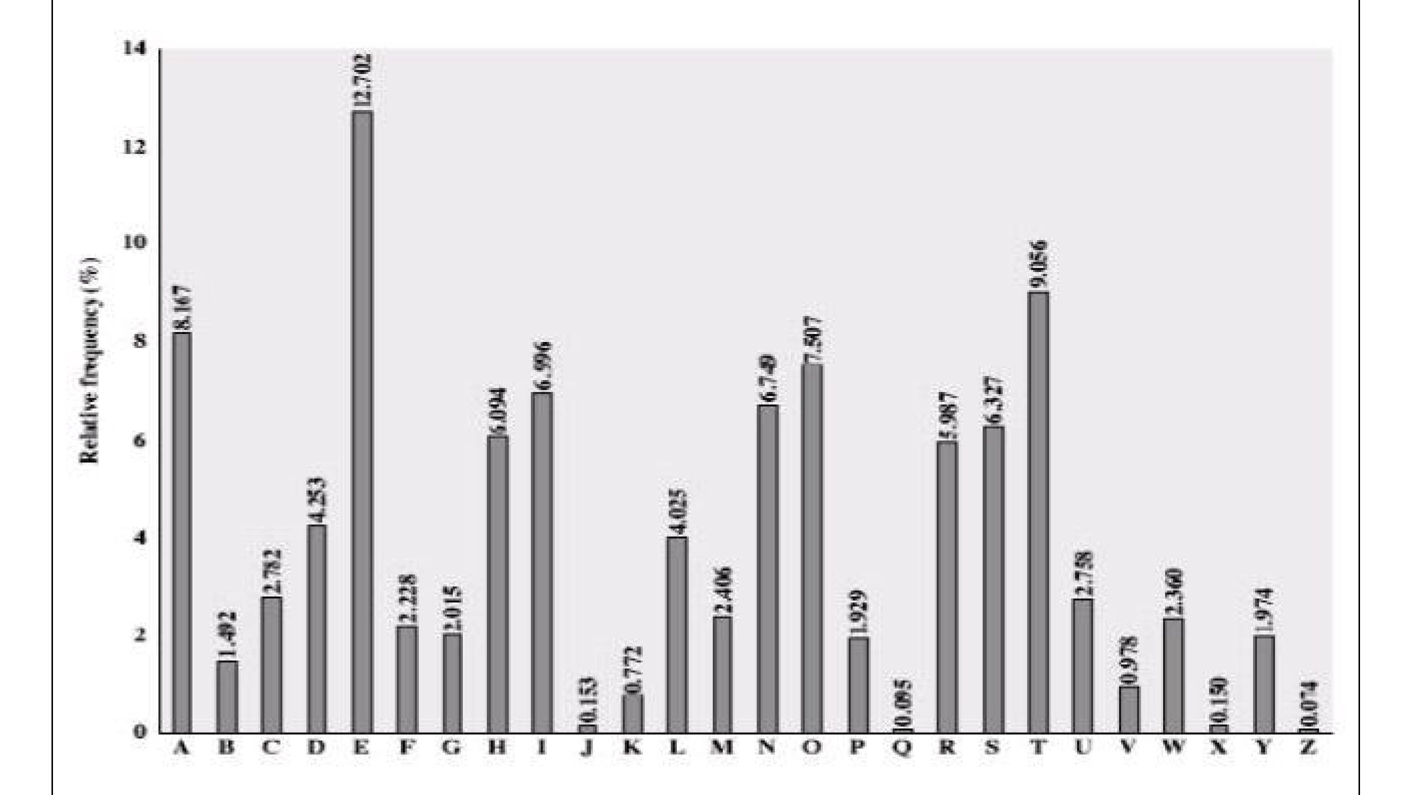
الحروف ليست متساوية في الاستخدام ، في اللغة الانجليزية على سبيل المثال E هو الأكثر استخداما ثم يأتي من بعده الحروف:

T, R, N, I, O, A, S

والحروف نادرة الاستخدام هي:

Z, J, K, Q, X

وهذا الجدول يوضح تكرار الحروف في اللغة Letters frequencies:



ولنأخذ على سبيل المثال النص التالي:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ.

ولمعرفة النص الناتج:

نحسب الحرف المتكرر في النص بأكبر تكرار.

على سبيل التخمين نجعل الـ P=e والـ Z=t .

وعلى سبيل التخمين أيضا ZW=th ومن ثم يكون ZWP=the.

و بعد المحاولات إلى أن نحصل على النص التالي:

it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in Moscow .

والآن ننتقل إلى الطريقة الثالثة وهي:

- **طريقة** Playfair :

أخترع هذه الطريقة العالم Charles Wheatstone في عام 1854م ولكنها سميت بعد ذلك بأسم صديقة Baron Playfair، وكانت هذه الطريقة تستخدم لعدة سنين بين(US & British) في الحرب العالمية الأولى (WW1).

وفكرة هذه الطريقة أن يكون لدينا مصفوفة من نوع 5x5، أي تكون المصفوفة مكونة من 25 عنصر ، ولكن الحروف الانجليزية تساوي 26 !!!

ولهذا السبب جعل Charles حرفي الـ **I** و J متساويان، أي(I<=I,J).

الشرح:

1. نختار مفتاح Key ولنفترض "COMPUTER".
2. نقوم بتعبئة المصفوفة ونبدأ بالمفتاح Key أولا .
3. بعد ذلك نكتب الحروف بعد المفتاح Key.
4. نبدأ بحرف ال A بعد كتابة المفتاح Key وبعده ال B ثم حرف ال C ولكن حرف ال C موجود في ال key ولذلك لا نكتب ال C بل نذهب إلى الحرف الذي بعده وهكذا إلى أن نصل إلى ال Z.

وتصبح المصفوفة Matrix كما يلي :

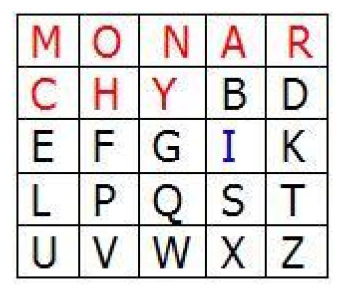
C	O	M	P	U
T	E	R	A	B
D	F	G	H	I
K	L	N	Q	S
V	W	X	Y	Z

طريقة التشفير:

لنأخذ مثال أخر :

المفتاحKey هو "MONARCHY".

وعند إكمال المصفوفة تصبح:



M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

1. نأخذ حرفين في كل مرة وإذا تشابه الحرفين نضع 'X' ، مثلا "balloon" تصبح كالتالي "ba lx lo on".

2. إذا جاء حرفين في نفس الصف مثلا "AR" (في الجدول السابق) نبدله مع الأيمن منه إلى "RM" وهنا وقعت في طرف الجدول أخذنا "R" ونرجع إلى بداية الصف ونأخذ ال "M". ولو جاء في الوسط مثلا : "ON" تصبح "NA" .

3. إذا جاء حرفين في نفس العمود ، نبدله مع الأسفل منه ، مثال "MU" يشفر إلى "CM" .

4. معادا ذلك (أي إذا وقعت الحروف غير المكان السابق) كل حرف يبدل مع الحرف الواقع في نفس العمود وعلى صف الحرف الأخر،مثال "HS" يشفر إلى "EA" , "BP" يشفر إلى "MZ", "IM" إلى "RU" وهكذا ..

ولفك التشفير نقوم بعكس الخطوات السابقة.

● **طريقة** Vigenere:

في هذه الطريقة نقوم بوضع مفتاح Key للنص على أن يكون :
- أن يكرر المفتاح Key على حسب طول النص.
- نجمع المفتاح Key مع النص الأصلي (نجعل كل حرف يساوي قيمته العددية) مثلا a=0 والـ2 = c وهكذا.

مثال :

باستخدام المفتاح (Key deceptive).

والرسالة Plaintext هي we are discovered save yourself .

نقوم بالآتي :

key: deceptivedeceptivedeceptive
plaintext: wearediscoveredsaveyourself

d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e
w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o	u	r	s	e	l	f
Z	I	C	V	T	W	Q	N	G	R	Z	G	V	T	W	A	V	Z	H	C	Q	Y	G	L	M	G	J

في المثال السابق:
1. قمنا بتكرار ال Key على طول النص الأصلي .

2. نجمع كل حرف من النص الأصلي مع الحرف الذي يوازيه من حروف المفتاح Key.

مثل : d+w وهي تساوي 3+22=25 وهو حرف ال Z اذا d+w=Z.

e+e تساوي 4+4=8 وهو حرف ال 8 I , I =.

وبعد تشفيرها يصبح النص :
ZICVTWQNGRZGVTWAVZHCQYGLMGJ

ولفك التشفير:

النص الأصلي = **النص المشفر – الحرف الموازي له من المفتاح** Key.

مثل Z-d أي 25-3 = 22 وال 22 تساوي حرف w. وهكذا...

و إلى هنا نصل إلى نهاية هذا الدرس وبالتالي نهاية الدورة وصلى الله وسلم على نبينا محمد..

ولا تنسونا من الدعاء .

****

النقاش والأسئلة

رابط النقاش: http://www.c4arab.com/showthread.php?threadid=26063

في طريقة Vigenere **إن كان المجموع أكبر من** 26 **فإننا على ما أعتقد سنقوم بالتدوير أليس كذلك؟**
وضح السؤال لو سمحت..

أقصد مثلا Z+C=29 **فالحل يجب أن يكون** (**برأيي**) **هو** C
أي.. C
وكيف أصبح:

مثل : d+w **وهي تساوي** 3+22=25 **وهو حرف ال** Z **إذا**.d+w=Z

أليس Z **رقمه** 26
في السؤال الأول: صح نبدأ من الأول إذا زاد عن 25.
z **يساوي** 25 **لماذا** : لأننا بدأنا من.a=0

في طريقة Vigenere **لنفرض أن النص الأصلي هو:**
we are discovered save yourself please
يعني تمت إضافة كلمة من : ستة حروف.
و المفتاح حروفه : تسعة .
فهل نضيف ستة حروف من المفتاح ؟
لا نضيف حروف على النص الأصلي بل المفتاح سوف يقف على الحرف السادس.

يوجد سؤال هل من الضروري الإعتماد على نفس القاعدة دون تغيير معطياتها مثلا الاحتفاظ بطريقة play fair **دون أن نغير المصفوف** 5 * 5 **؟**
هذه هي الطريقة.
وإذا أردت أن تعمل بطريقتك فلك هذا..

لى تعليق على طريقة play fair **فى التشفير**:
فلقد قمت من فترة صغيرة بتصميم برنامج تشفير يستخدم هذه الطريقة
ولكن مع بعض التطوير لإمكان إستخدامها فى تشفير ملفات و ليس نصوص فقط..
بمعنى بدلا من أن جدول الحروف 5*5 ، **أصبح** 16 * 16 = 256 **حرف و هم حروف الأسكى جميعا** ،
ويتميز أيضا بالسرعه المذهله فى التشفير/فك التشفير ، فتصل السرعه إلى 15 **ميجابايت فى الثانيه و يشفر جميع أنواع الملفات بإستخدام هذا الخوارزم البسيط**.
جزاك الله خير على التعليق

::: نقاشات عامة عن دورة أمن المعلومات :::

رابط النقاش: http://www.c4arab.com/showthread.php?threadid=26083

أستاذنا أبو سعد .. لقد ذكرت في النقطة الأولى لطريقة التشفير: Playfair
نأخذ حرفين في كل مرة وإذا تشابه الحرفين نضع 'X' , **مثلا** "balloon" **تصبح كالتالي.**"ba lx lo on"
هل هذه الكلمة هي من النص المراد تشفيره.. أم لا؟
أرجو أن توضح كيف تتم هذه الخطوة.. وإذا أمكن أن تعطينا مثال على..playfair **إذا سمحت..؟**
نعم هي من النص المراد تشفيره.
أنظري الجدول الأول واختاري أي نص وشفريه .. بالإعتماد على الطريقة كما هي مبينة في الجدول الثاني.

إذا ممكن توضيح كيف أصبحت balloon
ba lx lo on
هل أخذنا
ba
al
ll
lo
وهكذا .. أرجو التوضيح؟
أصبحت ال balloon بهذه الطريقة لوجود ال frequency في حرفي ال ll
ولاخفاء التكرار تصبح الكلمة:
ba lx lo on
أما كيف يتم أخذ الحروف فهو بهذه الطريقة:
نبدأ من الجهة اليسرى
نأخذ حرفين حرفين وإذا كانت متشابهة نفصلها ب x
فأولا :
ba لايوجد فيها شيء .
ثم
ll متشابهة نفصلها ب x وتصبح
lx ثم
lo هل هي متشابهة ؟ لا، ثم نكمل
on لا يوجد فيها شيء.

سؤال آخر .. لاحظت جميع المفاتيح المستخدمة في ..playfair **عدد حروفها** 8 **أحرف هل هذا شرط..؟؟**
كذلك هل يشترط أن تنتهي المصفوفة بحرف..z **؟؟**
ليس شرطا..
المفتاح ممكن يكون 8 أو أكبر أو أصغر..
مثلا لو كان المفتاح ZOO لن تنتهي بZ

هل يعتبر السيريال نمبر Serial Number **الموجود في البرامج أحد أنماط التشفير ؟**
لا.. لا تعتبر من التشفير !!..
لأن السيريال نمبر سهل كسره باستخدام بعض البرامج وتكون المعادلات والخوارزمية مخزنة في البرنامج.

قد لا تخلو أي معلومات أو نص من وجود أرقام خلالها...
هل تنقل الأرقام أو الرموز الخاصة من النص الأصلي إلى النص المشفر كما هي ؟
يحول الرقم الى نص .. مثلا 2 الى two وهكذا...

::: اختبار دورة أمن المعلومات :::

السؤال الأول:

(2) **أذكر سياستين أمنيتين من السياسات الأمنية** (**غير التي ذكرت في الدرس**)**؟**

السؤال الثاني:

2. **لماذا يفشل تطبيق السياسات الأمنية في الوطن العربي؟**

السؤال الثالث:

3.**قم بتشفير النص التالي:**

I love computer for Arab site

باستخدام كل من الطرق التالية:

(1) **طريقة** Caesar:

(2) **طريقة** Monoalphabetic **بالمفتاح** = (CXHTMYAUOLRGZNDKVQFIBJWPES):

(3) **طريقة** Vigenere **والمفتاح** = (course):

السؤال الرابع:

4.**قم بفك الشفرة للنصوص التالية:**

(2) Decrypt the following ciphertext, which is made with Playfair Cipher using " ieronymus" as the key. Blank spaces were first deleted and then inserted at convenient locations:

erohh mfimf ienfa bsesn pdwar gbhah ro

(2) The following ciphertext about President Kennedy was enciphered using a monoalphabetic substitution cipher. Blank spaces were first deleted and then inserted at convenient locations:

rgjjg mvkto tzpgt stbgp catjw pgocm gjs

~ انتهى الكتاب ولله الحمد والشكر ~

إن أحسنّا فمن الله.. وإن أخطأنا فمن أنفسنا والشيطان..
ولا تنسونا من صالح دعائكم